WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 5/00

A1

(11) International Publication Number: WO 00/00923

(43) International Publication Date: 6 January 2000 (06.01.00)

(21) International Application Number: PCT/US99/14894

(22) International Filing Date: 30 June 1999 (30.06.99)

(30) Priority Data:
09/107,746 30 June 1998 (30.06.98) US

(71) Applicant: @POS.COM, INC. [US/US]; 500 Oakmead Parkway, Sunnyvale, CA 94086 (US).

(72) Inventors: VALLIANI, Aziz; 1111 Tewa Court, Fremont, CA 94539 (US). KAREEMI, Nazim; 2145 Emerson Street, Palo Alto, CA 94301 (US).

(74) Agents: HERBERT, Thomas, O. et al.; Flehr Hohbach Test Albritton & Herbert LLP, Suite 3400, 4 Embarcadero Center, San Francisco, CA 94111-4187 (US).

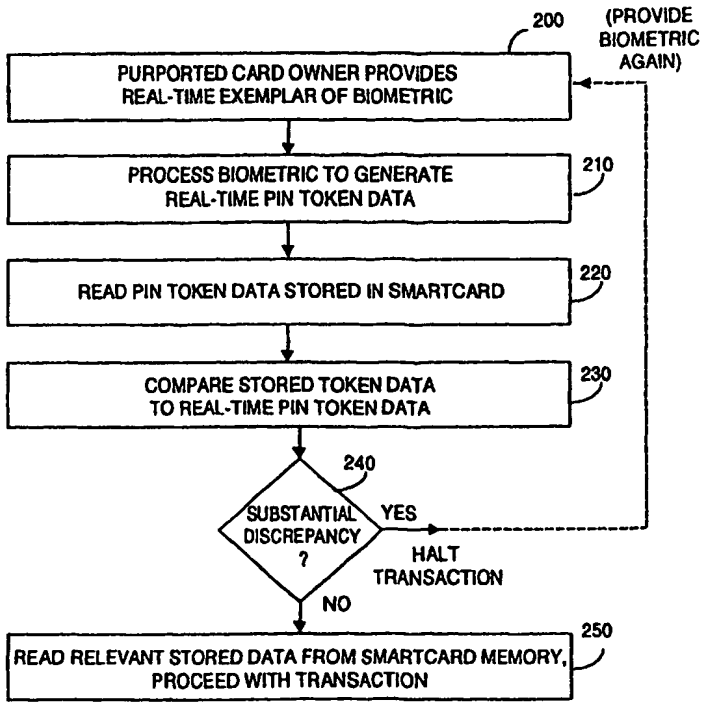
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: USER BIOMETRIC-SECURED SMARTCARD HOLDING DATA FOR MULTIPLE CREDIT CARDS

(57) Abstract

A smartcard securely stores confidential data, security is promoted by also storing within the smartcard memory a PIN token generated from biometric data provided by the cardholder. The biometric data may be any or all of a signature, a fingerprint, a voiceprint, and a video image, made by the cardholder, signal processed and stored securely in memory within the smartcard. When the smartcard is used in a transaction, access to the stored confidential data (250) is not allowed until the person presenting the card first recreates a biometric (200) substantially equivalent to what is represented by the memory-stored biometric PIN token (230).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

USER BIOMETRIC-SECURED SMARTCARD HOLDING DATA FOR MULTIPLE CREDIT CARDS

RELATIONSHIP TO PENDING PATENT APPLICATIONS

U.S. patent application 08/853,955 entitled "Modular Signature and Data Capture System and Point of Transaction Payment and Reward System", filed 9 May 1997 and assigned to the present assignee, discloses a flexible point of sale transaction terminal that may be used to practice the present invention.

FIELD OF THE INVENTION

This invention relates to systems and methods for securing confidential information, and more specifically to systems and methods to permit use of a smartcard to retain confidential data for multiple credit cards with security provided by at least one biometric provided by the smartcard owner.

BACKGROUND OF THE INVENTION

Credit cards and debit cards have found increasingly wide use in commercial transactions. A financial institution issues a card to a qualified user who uses the card to pay for merchandise and/or services during a transaction. As shown in Fig. 1A, for a credit or debit card 10, a magnetic stripe 20 on one surface of the card carries two or more tracks 30 of magnetically encoded data 40. The data identifies the card issuer and card account number. For a debit card, the card is issued with bank account identification data for the card owner. In use, the magnetically stored data is read and points to the user's account, from which it is determined whether the present transaction amount can be covered. Typically, cards that store data magnetically can at present only store about 200 bytes per card.

Fig. 1B shows a smartcard 50, which includes solid state memory 60 storing user data 70. Whereas magnetic storage on credit or debit cards is presently limited to perhaps 200 byes of data, memory 60 in smartcard 50 can store substantially more data. For example, data 70 may include any or all of bank account numbers, medical data, client names and telephone numbers, among other data.

Some individuals carry and use many different cards. Unfortunately carrying a few cards in one's wallet can render the wallet extremely bulky. Thus, there is a need for a method by which the bulk associated with carrying a plurality of cards can be substantially reduced.

Understandably the data stored in credit, debit, or smartcards (collectively "cards") must be maintained in a confidential manner, to prevent unauthorized charges against the subject account. One technique used to promote confidentiality of data stored in cards is to provide the card owner with a personal identification number ("PIN"), or password. When the card is being used during a transaction, the card user must manually enter the PIN on whatever device is used to read data from the card. If the card-stored PIN data agrees with what is now manually entered, the transaction can proceed, otherwise it will not proceed.

Unfortunately, card owners often forget their PIN. Other card owners may pick a PIN that is too easily compromised by a third party who somehow obtains the card, for example, a PIN that is simply the initials of the card owner. Thus, there is a need for a methodology that allows a card owner to reliably provide the correct PIN without memorization, which PIN cannot readily be compromised by third parties.

Further, there is a need for a system or method by which the equivalent of a plurality of cards can be implemented without undue bulk, while protecting data stored therein

with a PIN that need not be memorized and that cannot readily be compromised.

The present invention provides such a system and method.

SUMMARY OF THE PRESENT INVENTION

The present invention provides a single omnibus smartcard that can store data otherwise contained in at least two magnetically stored cards and/or at least one other smartcard. By storing multiple sources of data within a single smartcard, the bulk otherwise needed to store a plurality of cards is reduced.

To preserve confidentiality of data stored in the single omnibus smartcard, data representing a characteristic of the card owner is reduced to a token number that is also stored in the smartcard. This token number then represents the user's PIN. As such, there is no PIN that must be remembered by the user. The user characteristic preferably is a signature, but may be the user's fingerprint or voiceprint.

In the preferred embodiment, whenever the omnibus smartcard is used, the user provides a signature on a vendor's signature capture device. The capture device generates a token value from the signature. This real-time token value is compared with the true token value stored within the omnibus smartcard. If the two token values agree, the transaction can proceed. If they do not agree, the card user can be asked to provide a second signature to the vendor to re-check the token match. If there is no match, the transaction should not proceed. If the stored user characteristic is a fingerprint, when the smartcard is used the card user will provide a fingerprint to a fingerprint capture device that will generate a token value therefrom. If the stored user characteristic is a voiceprint, e.g., the user saying the user's name, when the smartcard is used, the card user

will enunciate the name into a voice capture device that will generate a token value therefrom.

In this fashion, data otherwise stored within a plurality of cards is storable within a single omnibus smartcard, with PIN-level security that does not require memorization of a PIN value, and that cannot readily be comprised by dishonest third persons.

Other features and advantages of the invention will appear from the following description in which the preferred embodiments have been set forth in detail, in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1A and FIG. 1B depict credit/debit and smartcards, respectively, according to the prior art;

FIG. 2 depicts an omnibus smartcard with enhanced PIN security, according to the present invention;

FIG. 3A depicts use of an omnibus smartcard according to a preferred embodiment of the present invention during a transaction; and

FIG. 3B depicts use of an omnibus smartcard according to alternative embodiments of the present invention during a transaction; and

FIG. 4 is a flowchart depicting steps carried out during a transaction using an omnibus smartcard, according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Fig. 2 depicts an omnibus smartcard 80 with enhanced PIN security, according to the present invention. By "omnibus" it is meant that smartcard 80 stores data that ordinarily would be stored in at least two separate cards (credit card, debit card, or smartcard) according to the

prior art. Smartcard 80 has an internal memory 90 that is shown storing data 40 (which may be identical to data 40 stored on a prior art credit card or debit card 10 as shown in Fig. 1A), data 40-1 (which may otherwise have been stored on another prior art credit or debit card such as card 10), data 70 (which may be identical to data 70 stored in a prior art smartcard 50 as shown in Fig. 1B), as well as data 70-1 (which might otherwise have been stored on another prior art smartcard such as card 50). For purposes of the present invention, it will be assumed that smartcard 80 stores at least 2 Kbytes of data, e.g., preferably more data than could be stored on a single prior art credit or debit card with magnetic data storage. Modern memory 90 can today store 8 Kbyte to 16 Kbyte, and future smartcard memory 90 will probably store at least 32 Kbyte. Regardless of its storage capacity, physically memory 90 is encapsulated within the body of card 80 per se.

Although Fig. 2 depicts omnibus smartcard 80 as storing data that would otherwise be stored in two credit/debit cards and two smartcards (e.g., a total of four cards), it is understood that the contents stored in memory 90 may include more or less than what would be stored in four prior art cards. Further, there is no need that memory 90 store data otherwise stored magnetically and in solid state, or that there be a 50%:50% proportion between the nature of what is stored in memory 90 in omnibus smartcard 80.

Note that omnibus smartcard memory 90 also stores cardholder characteristic data 100. According to the present invention, data 100 is a PIN value that must be re-generated at the time and place of a transaction involving omnibus smartcard 80. Rather than store a combination of numbers that the cardholder wishes (and must of course remember), data 100 is a digital token number that has been generated from a biometric or characteristic of the cardholder.

In the preferred embodiment the biometric will be the cardholder's signature, fingerprint, and/or voiceprint. Other potentially useful biometrics can include a scan of the retina of the cardholder, as well as a scan of the face of the cardholder.

When the cardholder first obtains an omnibus smartcard 80, the cardholder will provide the card issuer with a true exemplar of his or her biometric. Assume that the card will be issued by a local bank. The cardholder will go to the bank and provide a signature and/or a fingerprint and/or a voiceprint (e.g., enunciating the cardholder's name or some other word(s) that will be remembered). However, it is within the scope of the present invention that the biometric may include a retinal scan as well as a scan of the cardholder's face.

Using a signature biometric, note that as the cardholder writes the signature, the signature capture device captures relative amount of force used to write different portions of the signature, as well as relative time spent writing different portions of the signature. Such data is richer in biometric content than if a photocopy of signature were merely scanned electronically to generate a token.

The card issuer will electronically scan or otherwise process the cardholder-biometric exemplar to represent that data as a unique token number. Techniques for reducing a signature, or a portion of a fingerprint, or a voiceprint to a digital token representation are known in the art and need not be described in detail here. Suffice to say that for each instance of the same user's signature, fingerprint, or voiceprint, a token value may be generated. Although there may be some variations between signatures or voiceprints made by the same user at different times, the algorithm used to generate the signature or voiceprint token number will look at the common features, and will generate essentially the same

value each time. It is this signature, fingerprint, voiceprint (or indeed other reproducible cardholder biometric) token value that is stored as data 100 within omnibus smartcard 80, for use as a PIN during transactions made with the card.

It will be appreciated that one advantage of a signature, fingerprint, or voiceprint PIN token is that the cardholder need not memorize any number. All the cardholder must remember is to write his or her signature essentially the same way each time, or speak essentially the same each time, something most people do automatically. (In the case of a cardholder biometric that is a fingerprint, reproducibility of the fingerprint is essentially assured time after time.)

Because there is no PIN value for the cardholder to memorize (indeed the cardholder need never know his/her stored biometric PIN token), the PIN is not readily compromised. As will be seen, the only way a dishonest third party coming into possession of omnibus smartcard 80 can re-generate the relevant signature PIN value 100 is to perfectly forge the cardholder's signature or imitate the voice during the time of a transaction or somehow have a finger that will reproduce the cardholder's fingerprint.

Assume that the cardholder (or indeed a third party coming into possession of omnibus smartcard 80) wishes to make a transaction using the card. Referring to Fig. 3A, at the time and place of the transaction, the person presenting the smartcard will be asked to make a signature 110 using a stylus 120 upon the screen surface 130 of a signature capture device 140. An exemplary such signature capture device is the PenWare 3000, available from Mobilnetics Systems, Inc. of Delaware. Of course other such devices may instead be used.

Internal to or associated with device 140 will be electronics 150. Electronics 150 captures and signal processes the signature data from screen 130. Electronics 150 also executes an algorithm to represent the just-captured signature data as a real-time signature PIN token. Preferably the algorithm executed by or associated within device 140 will be similar to what was used to generate a signature PIN token such as is stored as data 100 within an omnibus smartcard, according to the present invention.

Before or after signature 110 is made during the transaction, the person intending to use smartcard 80 will causes the relevant portions of memory 90 to be read, e.g., preferably by device 140 or an equivalent device. Among the data to be read will be the actual signature PIN token data 100 that is known to represent the actual signature of the true owner of smartcard 80.

Electronics 150, which can be disposed within a host system 160 coupled to system 140 via a communications port 165, will now compare the genuine signature PIN token data 100 (read from card 80) with the just-generated signature PIN token data. If these two data are in substantial agreement, the subject transaction will go forward. Thus, relevant account data 40, or 40-1, or 70, or 70-1 will be read from memory 90 in smartcard 80, e.g., using device 140 (or the equivalent). The data read can be processed by remote host system 160 to make the transaction. In a commercial environment, device 140 will typically be at the cash register of a merchant's store, whereas system 160 may be the store's LAN computer system, or may be a remote databank-type system subscribed to by the merchant.

If, however, there is substantial disagreement between genuine signature PIN token data 100 and the just-generated signature PIN token data, further inquiry must be made. As noted, there is some signature-to-signature

deviation and the algorithm(s) used to examine the transaction can take such deviation into account. For example if the deviation appears to be just slightly out of the normal range of acceptance, electronics 150 can advise the merchant (e.g., through a message appearing on screen 130, or by audible beeps, etc.) to have the user re-sign his or her name on screen 130 for further analysis.

In some instances it may be desired to have the user produce a driver's license or other signature-bearing identification. If desired, system 140 could be augmented to permit document scanning of a signature, e.g., from the user's driver's license, for electronic comparison against the just-generated signature and/or against the true signature PIN token data 100. If desired, the document-scanned signature could be used to generate a third token value for comparison with genuine PIN token data 100.

Fig. 3B depicts the user of stored data 100 that represents a cardholder biometric that is a fingerprint, a voiceprint, a scan of the retinal portion of the cardholder's eye, and/or a scan of at least a portion of the cardholder's face. At the time and place of a transaction, the person presenting the smartcard will be asked to provide a fingerprint 170 upon a capture screen 175, and/or a voiceprint (shown as sound waves 180 emitted by the person 185 presenting the smartcard) detected by a microphone or the like 190 associated with an appropriate device 140'. For a retinal or face biometric, a TV camera or the like and associated electronics 195 will capture an image of the retina or face of the person 185 presenting the card. In a manner known in the art, the retinal scan or facial scan will be signal processed and reduced to an electronic token value. (In these embodiments, the cardholder would have presented himself or herself to the institution providing the smartcard, at which time the relevant biometric would have been cap-

tured, signal processed, and stored as compressed data 100 within memory 90 in smartcard 80.

Device 140' may be similar to device 140, except that it will now be augmented to capture fingerprints and/or soundwaves and/or video images for signal processing and reduction to a PIN token value.

Assume that electronics 150 captures and signal processes the fingerprint, voiceprint, or video (e.g., retinal scan or portion or all of a facial scan) data and also executes an algorithm to represent the just-captured data as a real-time fingerprint or voiceprint PIN token. Preferably the algorithm executed by or associated within device 140' will be similar to what was used to generate the fingerprint, voiceprint, or video PIN token such as is stored as data 100 within an omnibus smartcard, according to the present invention.

Similarly to what was above-described with respect to Fig. 3A, during the transaction, relevant portions of memory 90 are read from the smartcard, preferably by device 140' or an equivalent device. Among the data read will be the actual fingerprint, voiceprint, video PIN token data 100 that is known to represent the actual fingerprint or voiceprint of the true owner of smartcard 80.

As has been described, an electronic comparison is now made of the genuine fingerprint, voiceprint, video PIN token data 100 (read from card 80) with the just-generated fingerprint or voiceprint PIN token data. If these two data are in substantial agreement, the subject transaction will go forward, as was described. If, however, there is substantial disagreement between the genuine PIN token data 100 and the just-generated PIN token data, further inquiry will typically be made.

It will be appreciated that data 100 stored in memory 90 within smartcard 80 is not limited to a single biometric per user. For example, signature and fingerprint tokens may be compressed and stored in a few hundred bytes of memory each. Depending upon the storage capacity of memory 90, it is possible that all of the above-described parametrics could be stored for each user, or perhaps just two or three parametrics per user. It will be appreciated that if more than one user is permitted to use the smartcard, one or more appropriate parametrics per user may be stored within the smartcard memory.

Fig. 4 depicts the methodology practiced with the present invention. At step 200, the purported card owner must provide a real-time signature, fingerprint, voiceprint, or video image. As noted, this commonly would be done using an appropriate device such as shown in Fig. 3A or 3B. Typically at a point of transaction, perhaps a cash register area, the person using the card will write a signature, or provide a fingerprint, speak into a microphone, and/or allow a video image of his/her face or perhaps eye retina to be made.

At step 210, the just-generated biometric is scanned and/or signal processed electronically to generate real-time PIN token data. This real-time data will be the token-equivalent of the just-generated signature, fingerprint, voiceprint, and/or video image.

At method step 220, data 100 stored in smartcard 80 is read to access genuine PIN token data 100 stored within. At method step 230, a comparison is made, electronically, between the real-time PIN token data and the genuine signature, fingerprint, voiceprint, video image PIN token data read from the smartcard memory. This comparison, is preferably carried out by an algorithm executed by electronics 150, such as shown in Fig. 3B.

Next the results of the comparison is examined at method step 240. If there is no substantial discrepancy, the person presenting the smartcard is the smartcard owner whose signature, fingerprint, voiceprint, video image (or other parametric) PIN token data is stored within the smartcard. Using the present example, the transaction may proceed, and at step 250, the relevant data stored in smartcard memory 100 may be read, e.g., with a smartcard reader (or equivalent).

But if step 240 indicates is a substantial discrepancy, e.g., by flashing a message on screen 130 in device 140 (or an equivalent visual message on an equivalent device), or by audibly sounding a signal, the transaction should not automatically proceed without further investigation. As noted by the phantom line, it may be desired to have the person presenting the smartcard re-sign his/her name on the signature capture device, again provide a fingerprint 170, again speak into microphone 190 (being sure to enunciate the same words stored as a token in the smartcard), and/or again be video scanned with device 195. For example, the person may have been nervous and wrote a somewhat abnormal signature the first time at step 200. If this new signature (or other repeated biometric) now passes muster at step 240, the transaction may safely proceed. Otherwise, absent independent investigation of the bona fides of the person presenting the smartcard, the transaction should not proceed.

In short, it is seen that the present invention permits a single omnibus smartcard 80 to securely retain considerable data that otherwise would be stored in a plurality of cards that collectively are rather bulky. The use of the present invention need not be limited to commercial transactions. Further, data stored within the omnibus smartcard need not of course be limited to credit card account numbers, but may include (without limitation) medical records, confidential telephone numbers that can

only be read upon presenting a genuine signature to a device 140. For example, a corporation might issues omnibus smartcards 80 to key employees, wherein memory 90 stores confidential client data. Each smartcard 80 would also store genuine signature, fingerprint, voiceprint, video (and/or other biometric) PIN token data 100 for the card recipient. Thus, should the smartcard be lost or stolen, a third party could not gain access to the confidential data stored within.

To further promote confidentiality, it is understood that memory 90 may be fabricated so as to self-destruct in the event card 80 is broken into to gain physical access to memory 90. This may be accomplished by encrypting data stored in memory 90 with encryption keys maintained in memory 90, which keys are erased if the physical integrity of card 80 and/or memory 90 is violated. Techniques for protecting stored data in this fashion are known in the art and need not be further described herein.

It will also be appreciated that in some contexts, it may be desired that multiple users can share a single smartcard 80. In such instance, data 100 will include separate PIN token data for each individual user (be it signature, fingerprint, or both, PIN token data). During the course of a transaction (or course of gaining access to confidential data stored in memory 90), the relevant stored PIN token data 100 will be accessed, either because it is identical to the just-generated data, or because the user may be asked to enter his or her initials or employee number or the like as a pointer to the relevant stored PIN token data 100.

Modifications and variations may be made to the disclosed embodiments without departing from the subject and spirit of the present invention.

WHAT IS CLAIMED IS:

1. A method of securely storing confidential data relevant to a cardholder within a memory in a smartcard, comprising the following steps:

(a) storing within said memory said confidential data;

(b) storing within said memory PIN token data unique to said cardholder, said PIN token data representing a biometric created by said cardholder; and

(c) reading said confidential data from said memory only after a person presenting said smartcard provides a said biometric that upon signal processing, produces a PIN identical within a predetermined acceptance threshold to said PIN token data stored at step (b).

2. The method of claim 1, wherein at step (b) said biometric is a genuine signature made by said cardholder, and step (c) includes said person writing a signature, when using said smartcard, that upon signal processing produces a signature PIN identical within said predetermined acceptance threshold to said PIN token data stored at step (b).

3. The method of claim 1, wherein at step (b) said biometric is a portion of a fingerprint made by said cardholder, and step (c) includes said person producing a fingerprint, when using said smartcard, that upon signal processing produces a fingerprint PIN identical within said predetermined acceptance threshold to said PIN token data stored at step (b).

4. The method of claim 1, wherein at step (b) said biometric is selected from a group consisting of (i) a voiceprint made by said cardholder, (ii) a video image of at least a portion of a retina of said cardholder, and (iii) a video image of at least a portion of said cardholder's face.

5. The method of claim 1, wherein step (a) includes storing said confidential data in said memory in an encrypted format readable only with at least one encryption key also stored in said memory.

6. The method of claim 5, further including storing each said encryption key in said memory such that if physical integrity of said smartcard is violated, each said encryption key is erased;

wherein said confidential data stored in said memory is protected.

7. The method of claim 1, wherein said confidential data stored in said memory includes at least one type of data selected from a group consisting of (i) financial account data, (ii) business record data, (iii) business contact data, and (iv) medical data.

8. The method of claim 1, wherein:

said smartcard may be used by two cardholders;

at step (a) at least 4 KBytes of said confidential data is stored in said memory; and

step (b) includes storing unique PIN token data for each of said cardholders.

9. The method of claim 8, wherein step (a) includes storing confidential said data for use by each of said cardholders.

10. A smartcard that securely stores confidential data relevant to a cardholder within an internal memory, comprising:

memory having storage capacity for at least 4 KByte of confidential cardholder data whose confidentiality is to be preserved;

said memory further storing PIN token data unique to said cardholder, said PIN token data representing a biometric created by said cardholder;

wherein when using said smartcard, access to said confidential data is gained only after a person presenting said smartcard provides a said biometric that upon signal processing produces a PIN identical within a predetermined acceptance threshold to said PIN token data stored in said memory.

11. The smartcard of claim 10, wherein said memory further stores at least one encryption key such that said confidential cardholder data is stored in said memory in s format encrypted with said encryption key.

12. The smartcard of claim 11, further including means for deleting each said encryption key from said memory if physical integrity of said smartcard is violated.

13. The smartcard of claim 10, wherein said biometric is a genuine signature made by said cardholder, and wherein a person seeking to use said smartcard must first write a signature that upon signal processing produces a signature PIN identical within said predetermined acceptance threshold to said PIN token data stored in said memory.

14. The smartcard of claim 10, wherein:

said biometric is selected from a group consisting of (i) a portion of a fingerprint made by said cardholder, (ii) a voiceprint made by said cardholder, (iii) a video image of at least a portion of a retina of said cardholder, and (iv) a video image of at least a portion of said cardholder's face; and

a person seeking to use said smartcard must first produce a biometric that upon signal processing produces a PIN identical within said predetermined acceptance threshold to said PIN token data stored in said memory.

15. The smartcard of claim 10, wherein said confidential data stored in said memory includes at least one

type of data selected from a group consisting of (i) financial account data, (ii) business record data, (iii) business contact data, and (iv) medical data.

16. The smartcard of claim 10, wherein said smartcard may be used by two cardholders, and wherein said memory stores unique PIN token data for each of said cardholders.

17. The smartcard of claim 16, wherein said memory stores confidential said data for use by each of said cardholders.

18. A system for preserving security of confidential data relevant to a cardholder stored in a smartcard, comprising:

said smartcard including memory storing at least 4 KByte of confidential cardholder data whose confidentiality is to be preserved;

said memory further storing PIN token data unique to said cardholder, said PIN token data representing a biometric created by said cardholder; and

a unit, disposed at a point of use of said smartcard, with which a person presenting said smartcard must produce said biometric that upon signal processing produces a PIN identical within a predetermined acceptance threshold to said PIN token data stored in said memory before access to said confidential cardholder data is gained.

19. The system of claim 18, wherein said biometric includes at least one characteristic selected from a group consisting of (a) a genuine signature made by said cardholder, wherein said person presenting said smartcard must first write a signature that upon signal processing produces a signature PIN identical within said predetermined acceptance threshold to said PIN token data stored in said memory, (b) at least a portion of a fingerprint made by said cardholder, wherein said person presenting

said smartcard must first produce a fingerprint that upon signal processing produces a fingerprint PIN identical within said predetermined acceptance threshold to said PIN token data stored in said memory, (c) a voiceprint made by said cardholder, wherein said person presenting said smartcard must first enunciate at least one sound that upon signal processing produces a voiceprint PIN identical within said predetermined acceptance threshold to said PIN token data stored in said memory, and (d) a portion of a video image scanned from said cardholder, wherein said person presenting said smartcard must first be video scanned to produce an image that upon signal processing produces an image PIN identical within said predetermined acceptance threshold to said PIN token data stored in said memory.

20. The system of claim 18, wherein said smartcard may be used by two cardholders, said memory stores unique PIN token data for each of said cardholders, and said memory further stores confidential said data for use by each of said cardholders.

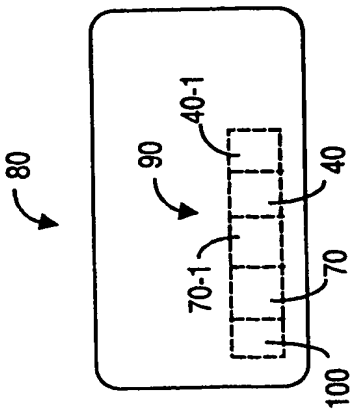


FIG. 2

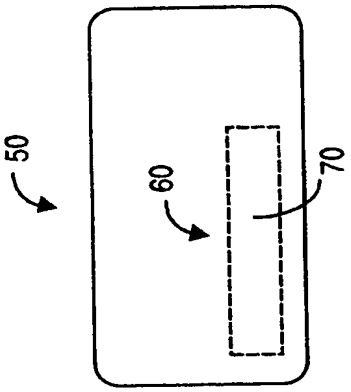


FIG. 1B
(PRIOR ART)

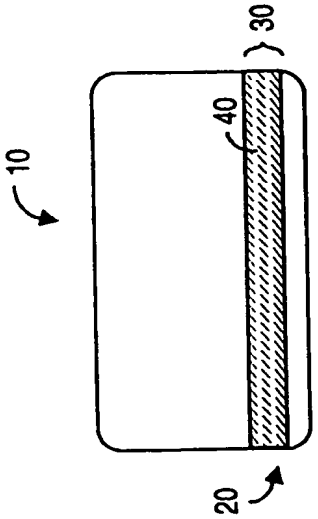


FIG. 1A
(PRIOR ART)

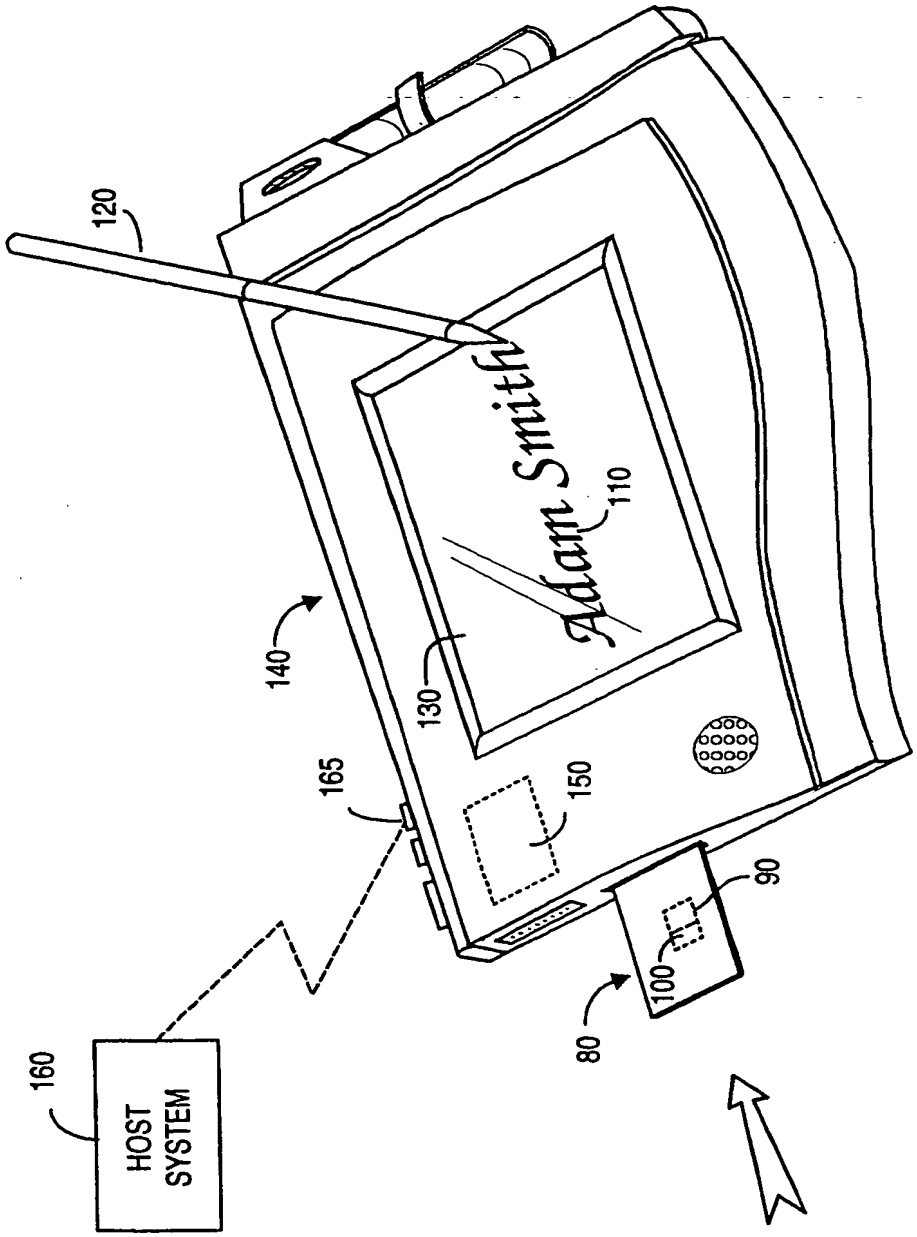


FIG. 3A

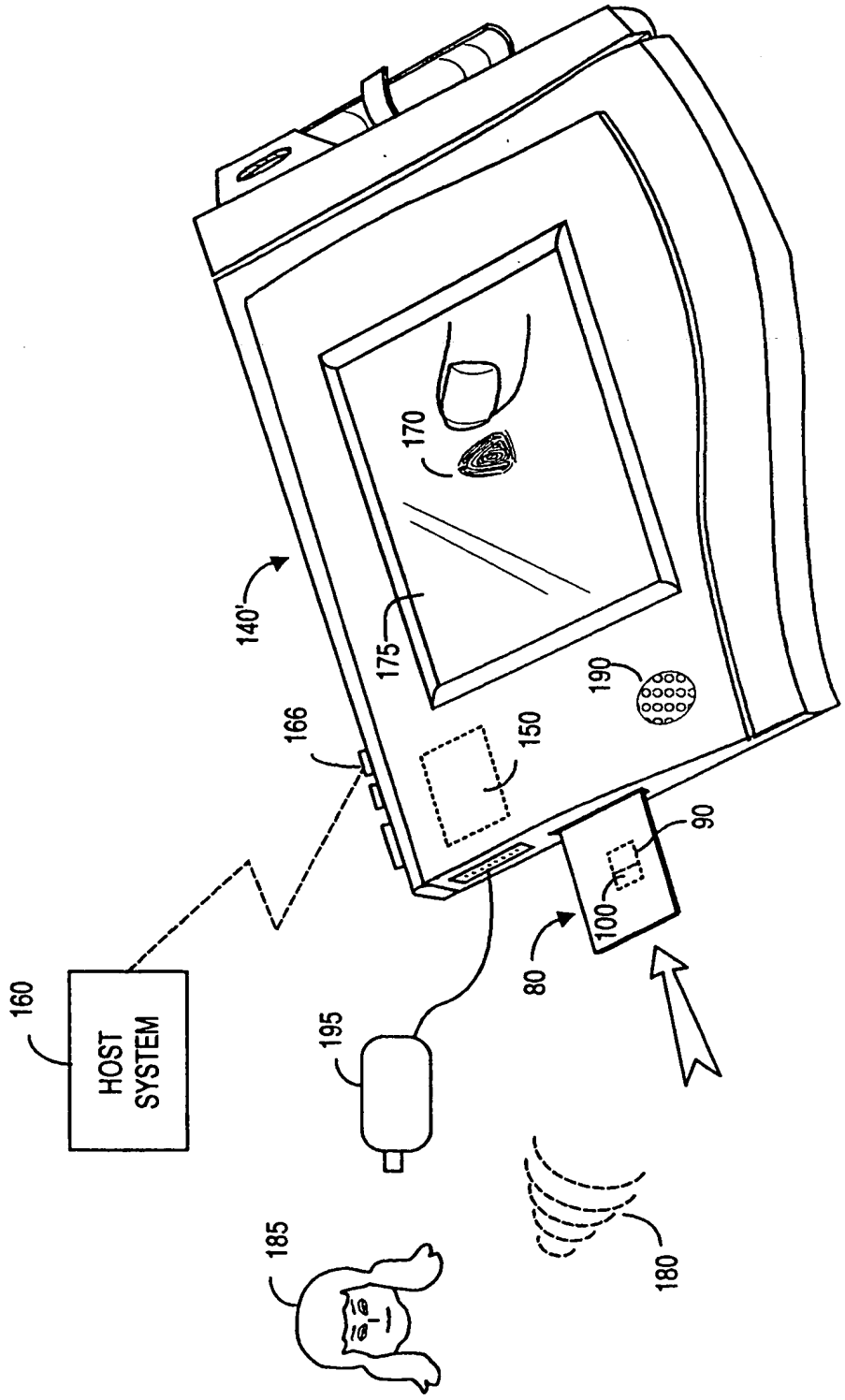


FIG. 3B

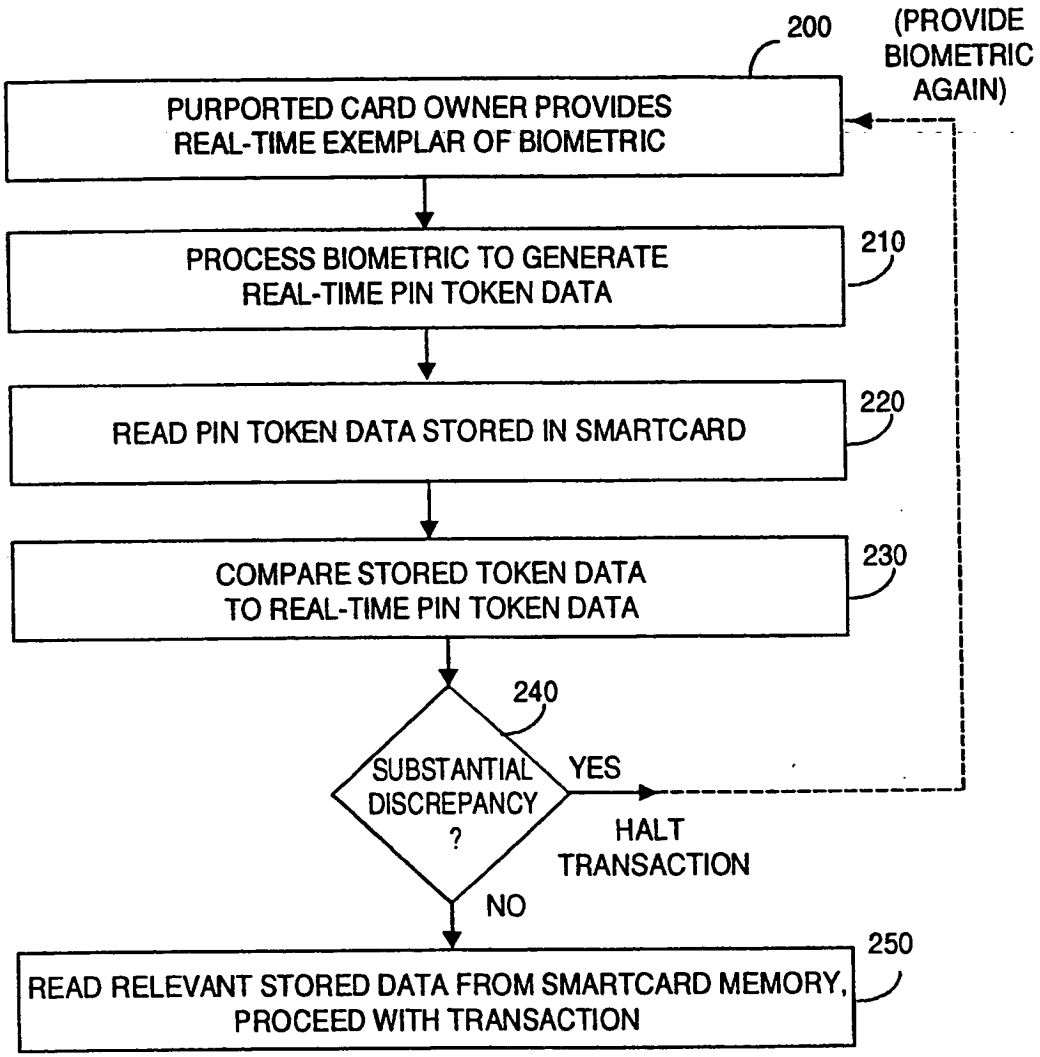


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/14894

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06K 5/00
US CL : 235/380

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 235/380, 382, 382.5, 492; 382/115, 117, 118, 119, 120, 124; 902/2, 3, 4, 5, 26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,578,808 A (TAYLOR) 26 November 1996 (26/11/96), see entire document.	1-7, 10-15, 18, 19
Y	US 4,827,518 A (FEUSTEL et al) 02 May 1989 (02/05/89), see entire document.	1, 10, 18
Y	US 4,837,422 A (DETHLOFF et al) 06 June 1989 (06/06/89), see column 1, lines 6-20, column 3, lines 32-52, column 4 lines 65-68, column 5, lines 1-34, column 6, lines 19-48, column 11, lines 26-31, column 12, lines 48-64.	8, 9, 16, 17, 20
Y	US 5,280,527 (GULLMAN et al) 18 January 1994 (18/01/94), see entire document, especially column 3, lines 37-55.	1-4, 7, 10, 13-15, 18, 19
Y	US 5,150,420 A (HARAGUCHI) 22 September 1992 (22/09/92), see entire document.	1, 2, 10, 13, 18, 19

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 AUGUST 1999	08 SEP 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JARED J. FUREMAN Telephone No. (703) 308-1782

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/14894

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,027,401 A (SOLTESZ) 25 June 1991 (25/06/91), see entire document.	1, 4, 10, 14, 18, 19
Y	US 4,993,068 A (PIOSENKA et al) 12 February 1991 (12/02/91), see entire document.	1-5, 7, 10, 11, 13-15, 18, 19
Y	US 4,700,055 (KASHKASHIAN, Jr) 13 October 1987 (13/10/87), see entire document.	None

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/14894

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

APS
search terms: IC card, smart card, chip card, memory card, circuit card, biometric, biometrics, fingerprint, signature, voiceprint, image, threshold, range, parameter, tolerance, limit, limits